Amendments to the Specification:

Please replace the paragraph starting on page 13, line 11, with the following amended paragraph:

Figure 3A is a diagram illustrating the usage protector 250 shown in Figure 2 according to one embodiment of the invention. The usage protector 250 includes a compressor 370, an encryptor 375, a storage 380, a decryptor 385, and a ~~compressor~~ decompressor 390.

Please replace the paragraph starting on page 13, line 33, with the following amended paragraph:

The encryptor 305 encrypts the first hash value 206 using the OSNK 203 to generate an encrypted first hash value 302. The encrypted first hash value 302 is then stored in the storage 310. Storage medium 310 may be any type of medium capable of storing the encrypted hash value 302. The storage medium 310 may ~~be any type of disk, i.e., floppy disks, hard disks and optical disks) or any type of tape, i.e., tapes~~ be, for example, a tape or a disk (e.g., a floppy disk, a hard disk, or an optical disk). At a later time, the subset 230 is tested for integrity. The decryptor 365 decrypts the retrieved encrypted first hash value 303 using the OSNK 203. This decrypting process generates a decrypted hash value 366. This decrypted first hash value 366 is then compared to the second hash value 312 by the comparator 315 to detect if changes have been made in the subset 230. If the two values match, then subset 230 has not been changed. If the subset 230 is deliberately updated by an authorized agent, the stored encrypted hash value is also updated, and a subsequent integrity test again results in the two hash values (366 and 312) matching. If the subset 230 is modified by an unauthorized agent that does not update the stored encrypted hash value, then the subsequent integrity test results in differing hash values 366 and 312, signaling the unauthorized modification. The unauthorized agent cannot avoid this detection by attempting to generate its own

version of the stored encrypted hash value, because the unauthorized agent does not have access to the OSNK 203.

Please replace the paragraph starting on page 16, line 15, with the following amended paragraph:

Figure 3E is a diagram illustrating the usage protector 250 shown in Figure 2 according to another embodiment of the invention. The usage protector 250 includes a first encryptor 305, a second encryptor ~~365~~ 311, a storage medium 310, and a comparator 315.

Please replace the paragraph starting on page 16, line 19, with the following amended paragraph:

The first encryptor 305 encrypts the first hash value 206 using the OSNK 203. The first hash value 206 is provided by the hashing function 220 as shown in Figure 2. The first encryptor 305 takes the first hash value 206 and encrypts it to generate an encrypted first hash value 302 using the OSNK 203. The encrypted hash value 302 is then stored in a storage 310 for later use. The encryption by the OSNK 203 allows the encrypted first hash value 302 to be stored in arbitrary (i.e., unprotected) storage media. Storage medium 310 may be any type of medium capable of storing information (e.g., the encrypted hash value 302). The storage medium 310 may ~~be any type of disk, i.e., floppy disks, hard disks, and optical disks) or any type of tape, i.e., tapes~~ be, for example, a tape or a disk (e.g., a floppy disk, a hard disk, or an optical disk). The second encryptor ~~365~~ 311 encrypts the second hash value 312 to generate an encrypted second hash value 301 using the OSNK 203. The second hash value 312 is provided by the hash function 220. The first encryptor 305 and the second encryptor ~~365~~ 311 use the same encryption algorithm, and this algorithm produces identical repeatable results for a given input. The encrypted first hash value 302 is now retrieved from the storage 310 for comparing with the encrypted second hash value 301. The comparator 315 compares the encrypted second hash value 301 with the retrieved encrypted first hash value 303 to detect if the subset 230 has been modified or tampered with. In the case where the subset 230 is

deliberately updated by an authorized agent, the stored encrypted hash value is also updated. Since the modification of the subset 230 is authorized, the second encrypted hash value 301 is the same as the retrieved first encrypted first hash value 303. In the case where the subset 230 has been unauthorized modified or tampered with, the comparator 315 generates a modified/not-modified flag indicating the subset 230 has been modified and therefore, the subset 230 should not be used. An attacker cannot simply replace the first encrypted hash value 303 with one corresponding to the unauthorized modified subset 230, because the attacker does not have access to the OSNK 203 used to encrypt the hash value.